Statement of Work (SOW) for
Ashore & Afloat Risk Management Framework Accreditation, Validation, Cyber Security, Quality Assurance, Engineering and Technical Writing Support

1.0 INTRODUCTION

1.1 The Naval Surface Warfare Center Philadelphia Division (NSWCPD) is a Department of Defense (DoD) entity responsible for HM&E research and development, test and evaluation, engineering and fleet support organization for the Navy's ships, submarines, military watercraft and unmanned vehicles. This requirement is for NSWCPD Code 50 which is responsible for multiple technical branches in support of Risk Management Framework (RMF) package development to ensure systems receive full Authority To Operate (AO), RMF System Validation of those associated packages and provide Cyber Security and Information Assurance (IA) Harding of Ashore and Afloat systems.

1.2 This contract is for non-personal services. It does not create employment rights with the U.S. Government whether actual, inherent, or implied

1.3 Government / Contractor Relationship

(a) The services to be delivered under this Task Order are non-personal services and the parties recognize and agree that no employer-employee relationship exists or will exist under the Task Order between the Government and the Contractor's personnel. Therefore, it is in the best interest of the Government to provide both parties a full understanding of their respective obligations.

(b) The Contractor employees shall identify themselves as Contractor personnel by introducing themselves or being introduced as Contractor personnel and displaying distinguishable badges or other visible identification for meetings with Government personnel. In addition, Contractor personnel shall appropriately identify themselves as Contractor employees in telephone conversations and in formal and informal written correspondence.

(c) Contractor personnel under this Task Order shall not engage in any of the inherently Governmental functions listed at FAR Subpart 7.5 or DFARS Subpart 207.5.

(d) Employee Relationship:

1) The services to be performed under this Task Order do not require the Contractor or its personnel to exercise personal judgment and discretion on behalf of the Government. Rather the Contractor's personnel will act and exercise personal judgment and discretion on behalf of the Contractor.
2) Rules, regulations, directives, and requirements that are issued by the U. S. Navy and NSWCPD under its responsibility for good order, administration, and security are

applicable to all personnel who enter a Government installation or who travel on Government transportation. This is not to be construed or interpreted to establish any degree of Government control that is inconsistent with a non-personal services contract.

(e) Inapplicability of Employee Benefits: This Task Order does not create an employer-employee relationship. Accordingly, entitlements and benefits applicable to such relationships do not apply.

(f) Notice. It is the Contractor's, as well as the Government's, responsibility to monitor Task Order activities and notify the Contracting Officer if the Contractor believes that the intent of this Section has been or may be violated.

1) The Contractor shall notify the Contracting Officer in writing via letter or email within three (3) calendar days from the date of any incident that the Contractor considers to constitute a violation of this Section. The notice should include the date, nature, and circumstances of the conduct; the name, function, and activity of each Government employee or Contractor official or employee involved or knowledgeable about such conduct; identify any documents or substance of any oral communication involved in the conduct; and the Contractor's estimated date when, absent a response, cost, schedule or performance will be impacted.
2) The Contracting Officer will, within five (5) calendar days after receipt of notice, respond to the notice in writing. In responding, the Contracting Officer will either:
    i. Confirm the conduct is in violation and when necessary direct the mode of further performance,
    ii. Countermand any communication regarded as a violation,
    iii. Deny that the conduct constitutes a violation and when necessary direct the mode of further performance, or
    iv. In the event the notice is inadequate to make a decision, advise the Contractor what additional information is required, and establish the date by which it should be furnished by the Contractor.

2.0 BACKGROUND

NSWCPD Department 50 is responsible for cybersecurity support across multiple ship systems and platforms, and continues to improve its overall cybersecurity posture utilizing the latest in security assessment tools, patch management, image development and processes to achieve the most secure systems possible. Cybersecurity Professionals support ashore and afloat systems working closely with engineering teams to implement cybersecurity measures to increase Fleet readiness. Integration across multiple platforms is key to cyber awareness.

There is a requirement to identify and properly manage the risk of Navy Information Technology (IT) in accordance with the DoD Instruction (DoDI) 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT). RMF uses a risk-based cybersecurity approach for enterprise-level authorization of IT systems and services. The RMF implements and enforces a tailored set of security controls, NIST Special Publication 800-53 Revision 4 and CNSSI 1253, and focuses on security as an integral part of a system’s overall lifecycle. RMF facilitates assessment and authorization (A&A) in order to attain an Authority to Operate (ATO). In addition, DoD Information Technology (IT) mandates the management of cybersecurity through RMF by applying the RMF process and integrate cybersecurity into the acquisition and systems engineering processes for NAVSEA Platform Information Technology Control (PIT-Control) systems. Adaptation of the National Institute of Standards and Technology (NIST) RMF in NIST Special Publication 800-37 Revision 1. T

Programs currently supported by Dept 50 include, Instrumentation and Sensor Systems; HM&E Control Systems (of the following classes: DDG 1000, LCS, LDP; CVN; DDG 51; CG, LHA, LHD; LSD, FFG, and MCM), New System Development, Advanced Damage Control Systems, Fluid System Automation, New Construction & LBES Integration, In-Service Engineering, Machinery Automation, Machinery Control Systems, Remote Monitoring and Condition Based Maintenance Systems, Acquisition & Information Systems, HM&E Navigation Networks, Ship Navigation Integration Bridge Systems and Navy ECDIS Controls, Ship Controls & Navigation CVN & New Development, Ship Controls Surface Combatants, Ship Controls Amphibious and Ship Instrumentation & System Calibration.

3.0 SCOPE OF WORK

Contractor support is required for performance across multiple ship classes, shipboard and shore-based systems and subsystems in the areas of Cybersecurity, Engineering Support, Engineering Logistics Support, Quality Assurance Support, Technical Documentation, RMF and System Accreditation. The target platforms are primarily U.S. Navy Surface Ships, Carriers, Submarines and Service Craft. In addition to the Active and Reserve U.S. Navy ships, this contract will also support HM&E upgrades on Army watercraft, Coast Guard vessels, Foreign Military Sales (FMS) platforms, Military Sealift Command (MSC) vessels, National Oceanic and Atmospheric Administration (NOAA) Vessels, land-based test sites, and other DOD platforms. RMF requires the consistent monitoring and maintenance as well as overall sustainment of the security posture of the IT systems.

In addition to the development of Cybersecurity and Engineering, the Navy also requires that multiple ship classes and their associated systems and subsystems be certified and accredited in accordance with the DoD Information Assurance Certification & Accreditation Process (DIACAP) using the RMF. Certification & Accreditation (C&A) also applies to the IT information, systems, artifacts, and relevant data that are generated by a system-lab-owner (i.e. Information Systems Security Engineer (ISSE)/Information System Owner (ISO) who facilitates C&A via Naval Sea Systems Command (NAVSEA) and Operations Designated Accredited Authority (ODAA)).

Cybersecurity solutions necessitate the satisfaction of requirements in adherence and compliance with Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) and Security Requirements Guides (SRGs). Secure-system-configuration and hardening entails Assured Compliance Assessment Solution

(ACAS) vulnerability assessments, anti-virus (AV) scanning, and certifying-activities to demonstrate and prove a system's capability and reliability within a secure environment.

Along with the certifying activities, the Navy requires validation of those associated systems and subsystems in order to obtain Authorization to Operate (ATO). A&A packages must be reviewed and verified prior to issuance of ATOs to ensure complete compliance with the DIACAP/RMF.

4.0 APPLICABLE DOCUMENTS

4.1 DoD Instruction 8510.01, Subj: Risk Management Framework (RMF) for DoD Information Technology (IT) dated 12 March 2014 takes effect per NAVSEA guidance.
4.2 Certification and Accreditation (C&A) Requirements for DoD-wide Managed Enterprise Services Procurements, DoD Chief Information Officer memorandum dated Jun 22, 2006
4.3 DON CIO Memo 01-09, Information Assurance Policy for Platform Information Technology dated 30 Jan 2009
4.4 NAVSEAINST 9400.2, Implementation of Naval Sea Systems Command (NAVSEA) Afloat Information Assurance (IA) Governance and Guidance dated 18 Aug 10
4.5 DoDD 8500.01x, Information Assurance
4.6 DoDI 8500.2x, Information Assurance Implementation
4.7 DODI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP) dated 28 Nov 2007
4.8 DODD 8570.01, Information Assurance Training, Certification, and Workforce Management
4.9 DoD 8570.01-M, Information Assurance Workforce Improvement Program
4.10 DoD 8140.01 “Cyberspace Workforce Management requirement
4.11 NIST 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004
4.12 Navy Certification Agent Qualification Standards and Registration Guidebook, v.
4.13 Navy Enterprise Mission Assurance Support Service (eMASS) User Guide – Validator, U.S. Fleet Cyber Command, Office of the Navy Operational Designated Accrediting Authority (ODAA), Version 1.1, 2 July 2012.
4.14 OPNAV 5239.3B, DON IA Policy dated 17 June 2009
4.15 NAVSEAINST 2200.1, Use of portable electronic devices (PEDs) at the Naval Surface Warfare Center, Philadelphia Division (NSWCPD) dated 02 Feb 2015
4.16 NAVSEA 5239.2A, NAVSEA IA Program dated 15 Dec 2008

These documents can be referenced at: www.navsea.navy.mil & www.nist.gov

The Contractor shall reference and utilize the latest version available when performing tasks within this SOW.

5.0 REQUIREMENTS

5.1 **CYBERSECURITY**

5.1.1 **SERVER ADMINISTRATIVE SUPPORT**

NSWCPD requires installation, configuration, and integration of new technology with IT security standards; file backups; security patches; and the performance of analysis to ensure security controls are properly implemented. Operating systems include multiple variants of Linux/UNIX, Microsoft Windows server, workstation and VMware operating systems. The Contractor shall:

5.1.1.1 Install, configure, troubleshoot, resolve, and execute backup of:

- 5.1.1.1.1 Linux/UNIX Consoles
- 5.1.1.1.2 Windows Server/Workstation Consoles
- 5.1.1.1.3 VMWare/ Hyper-V Virtual Infrastructure
- 5.1.1.1.4 Storage Area Networks
- 5.1.1.1.5 Database Servers

5.1.1.2 Register users for servers associated with network operations and Enterprise application access.

5.1.1.3 Install security patches on servers to eliminate identified vulnerabilities, and report on patch compliance in accordance with CDRL A005.

5.1.1.4 Perform routine audits of systems and software; add, remove, and/or update user account information and perform password-resets, as applicable in accordance with the latest Roster List.

5.1.1.5 Monitor system-security to maintain security posture, and document the latest version of system-configuration in accordance with CDRL A005.

5.1.1.6 Conduct performance tuning – tasks include optimization of equipment and devices to ensure performance of parts and systems is as close to their theoretical peaks as possible.

5.1.1.7 Research and recommend methods and procedures to implement new security patches and remediation; recommendations shall be provided in accordance with CDRL A005.

5.1.2 **CYBERSECURITY DESKTOP ADMINISTRATIVE SUPPORT**

To accomplish this management task, the contractor shall perform the following:

5.1.2.1 **Configuration Management**

The Contractor shall implement configuration version control practices and processes (i.e. checkout/check-in; version number control; system/software baselines; merge, build, test, and release) for software, hardware, firmware, images, technical manuals, test procedures and other support documentation.

5.1.2.2 **Desktop Support**

Troubleshoot user-problems to determine whether the issues are hardware, software, procedural, or communication-related and route the issue/problem to the correct support-party for resolution; Contractor shall track and log the incoming requests and report the incidents.

5.1.2.3 **Troubleshoot**

Provide first-level usage support for locally developed applications deployed within Department 50.

5.1.2.4 **Assess**

Monitor desktop systems on a daily basis to discover/find, and correct any identified technical problems.

5.1.2.5 Hardware

Install devices on the network, to include activating the network port; configuring the device to be compatible with the network; ensuring compatibility with the latest standard software configuration; and update NSWCPD-databases with the device information.

5.1.2.6 **Monitor**

Plan and coordinate security measures to safeguard information in computer files against accidental or unauthorized damage, modification or disclosure. Recommendations for implementation shall be presented to NSWCPD.

5.1.2.7 **Evaluate**

Plan and support the installation and testing of new products and improvements to computer systems, such as the installation of new databases. Recommendations for implementation shall be presented to NSWCPD. If approved, Contractor shall coordinate and schedule the approved installations.

5.1.2.8 **Manage**

Plan and design the implementation of database-management-software to add, delete, and update user information in accordance with NAVSEAINST 9400.2 policy and regulation.

5.1.2.9 **Procedures**

Develop and prepare implementation-and-maintenance, access control, inventories, and communications-documentation, as well as Standard Operating Procedures (SOPs).

5.1.3 **POLICY AND PORTFOLIO MANAGEMENT/RDT&E GOVERNANCE SUPPORT**

NSWCPD is responsible for ensuring its current and future IT systems abide and comply with Federal and DoD regulations. To support NSWCPD with this requirement, the Contractor shall:

5.1.3.1 **Preparation**

Research and provide guidance on the latest scientific and engineering community discoveries with respect to cybersecurity and encryption of information for more secure networking and operational-security. Findings shall be presented in accordance with CDRL A004.

5.1.3.2 **Research**

Analyze the potential impacts of implementing new policies in the DoD environment as they relate to regulations such as the Clinger-Cohen Act, Federal Information Security Management Act (FISMA), Section 508, and Federal Information Processing Standards (FIPS). Findings shall be presented in accordance with CDRL A004.

5.1.3.3 **Advise**

Recommend strategies and courses of action that specifically address improved mission capabilities, data migration, capacity planning, systems/infrastructure engineering, and related support activities.

5.1.3.4 **Documentation**

Assist in the preparation of high-level policies and/or strategies for Information Assurance:

Summaries and White papers

5.1.3.4.1 Presentations

5.1.3.4.2 User manuals

5.1.3.4.3 Administrative Guides

5.1.4 CYBERSECURITY INFORMATION ASSURANCE / NAVY INFORMATION DOMINANCE APPROVAL SYSTEM (NAVIDAS) PROGRAM SUPPORT

To accomplish this management task, the contractor shall perform the following:

5.1.4.1 **Manage**

Support milestone and issue tracking; document and log initiations/requests and associated activities and report them

5.1.4.2 **Monitor**

Administer and manage website content in accordance with (NIST) security control standards.

5.1.4.3 **Administrator**

Coordinate and schedule program reviews - Contractor shall maintain master project calendar and coordinate arrangements for presentations/meetings; Contractor shall maintain Plan of Action and Milestones (POA&M)

5.1.4.4 **Document**

Assist in the creation and preparation of technical documentation such as user manuals, reports, outlines, and summaries.

5.1.4.5 **Coordinate**

Update and manage software libraries in accordance with (SOP) procedures, and execute the destruction of dated versions in accordance with DoD mandates.

5.1.4.6 **Analyze**

Review NAVIDAS Purchase Requests against DoN Policies and regulations; and provide comments regarding the submission's compliance with the aforementioned policies and regulations.

5.1.4.7 **Audit**

Update NAVIDAS checklists and guidebooks to help streamline the processing of future IT Purchase Requests

5.1.4.8 **Account**

Support network account information on System Access Authorization Request (SAAR) forms track, update and cross verify all users with access to identified systems have approved SAAR.

5.1.4.9 **Security**

Media Transfer Agent - ensure that personnel transferring classified data to removable media have the proper training and approval to perform Media Transfer Agent-functions in accordance with NAVSEA 09P and that personnel designated as Media Transfer Agent have appropriate security clearance in accordance with the Contract DD Form 254 Contract Security Classification Specification

5.2 CYBERSECURITY TECHNICAL WRITING

The contractor shall write technical documentation such as user manuals, reports, documentation, presentations, proposals, outlines, and summaries in support of both ashore and afloat systems across multiple platforms. Support develop of technical documents across multiple platforms including configuration management, milestone, issue tracking, web site content management and RMF documentation.

5.2.1 The Contractor shall perform a detailed technical documentation analysis of the software/hardware associated with the system and components.

5.2.1.1 The technical writer shall develop system architecture diagrams, software design requirements, network connection diagrams, integrity analysis of integrated products, life-cycle management analysis, and vulnerability assessment.

5.2.1.2 Based on this analysis, the contractor shall write, remediate and mitigate security vulnerabilities resulting from the software development tools used, operating system deficiencies, and the actual software implementation.

5.2.2 Create and maintain a vulnerability Navy eMASS POAM for systems. Contractor shall have access to the Navy eMASS system classified and unclassified.

5.3 ENGINEERING SUPPORT

5.3.1 ENGINEERING ANALYSIS

5.3.1.1 **Ship Checks**

Assist with onboard ship evaluation and assessments in preparation for the execution of system installations and upgrades. Duties include reviewing existing drawings, verification of equipment locations, determining cable management requirements and interfacing with the applicable Planning Yard to support Ship Installation Drawing development.

5.3.1.2 **Technical Data Packages**

Assist with the development of Technical Data Packages in relation to the planning and execution of shipboard alterations. Duties include the creating of Functional Block Diagrams, Wiring Tables, Equipment Specifications and Interface Design Documents. (CDRL A014)

5.3.1.3 **Ship Installation Drawing Reviews**

Assist with the review of Ship Installation Drawings received from the Planning Yard. Duties include verifying that the Ship Installation Drawings are accurate and reflect the guidance provided from the Technical Data Package. (CDRL A014)

5.3.1.4 **Failure Review Boards**

The Contractor shall assist with the preparation and support of Failure Review Boards. Duties include participating in any associated technical or project related teams. Also, tasks include the compiling of existing system documentation, development of risk assessments and failure analysis reporting.

5.3.1.5 **Specification Reviews**

5.3.1.5.1 Identify applicable DoD and DoN source documents related to system components, maintenance, repair, upgrades and manning requirements.

5.3.1.5.2 Develop assessment *I* evaluation protocol for shipboard assessments. Assessments include, but are not limited to corrosion and structural integrity.

5.3.1.5.3 Support development and review of system and equipment specifications. Duties include developing and updating specifications due to system modifications. Also, the review of all specifications for technical accuracy is required.

5.3.1.6 **Fleet Support Coordination**

5.3.1.6.1 Provide engineering technical and logistic support as required. Review, update, and/or develop Integrated Logistics Support (ILS} Certifications and Operating Materials & Supplies (OM&S).

5.3.1.6.2 Review, update, and/or develop supporting logistics documentation (Technical Manuals, Planned Maintenance Systems, Approved Products Lists, Drawings, etc). Develop recommendations on corrective actions and recommendations to prevent future system failures.

5.3.1.6.3 Develop, update, and maintain a database for all materials engineering technical efforts.

5.3.1.6.4 Participate in meetings as requested to understand fleet concerns and improve logistics readiness. Classify, inventory and maintain data of OM&S material in ERP.

5.3.1.6.5 Support coordination efforts in relation to Fleet assistance requests. Specific details on the request; tracking hours expended and follow-up communication until the issues are resolved. Fleet support requests associated to system failures, operational questions, maintenance support, supply support and logistics updates.

5.3.2 ENGINEERING TRAINING COORDINATOR

5.3.2.1 Design ~~and develop software processes and~~ procedures related to testing, troubleshooting, and training in accordance with the organization's standard processes. ~~(CDRL A017)~~

5.3.2.2 Perform shipboard and in-shop technical assistance / training for operation, maintenance, test, repair alteration, modification, and upgrade of machinery systems and software. Conduct on-the-job training for ship's personnel in documentation, operation and maintenance of software.

5.3.2.3 Provide technical information and perform documentation updates to associated system training materials for Government review.

5.3.2.4 Perform requirements analysis, programming, system documentation, maintenance and training for control systems, including but not limited to, developing functional descriptions, systems design, systems specifications, data dictionaries, and user documentation.

5.3.2.5 Contractor assessments to develop an action plan for improvement; direct workshops to implement process improvement or critical special projects, including common process definition and mapping; and provide leadership training and executive coaching workshops

5.3.3 ENGINEERING SYSTEMS TECHNICIAN

5.3.3.1 System Troubleshooting

The Contractor shall participate in system assessment and evaluation in relation to reported issues from the Fleet. Duties include:

1) Evaluation of Material Failures in HM&E Systems and Components
    a. Provide engineering technical support and procure materials necessary for the evaluation of system and component failures resulting from the improper selection or improper use of materials, or their manufacturing.
    b. Assess current system design and configurations associated with failures.
    c. Conduct root-cause analysis of system failures. Utilize destructive and non-destructive evaluation (NOE) as part of tool set for evaluation. Replicate the issue in a land based test facility and validate potential resolutions.
        i. Shipboard support could be required to assist Ship's Force and Regional Maintenance Centers with the determination of the root cause.

5.3.3.2 Land Based Test Site Support with the continued operation and maintenance of land based test sites. Duties include:

1) Configuring equipment to support system testing and fleet support validation efforts.
2) Liaison Action Requests (LARs)
    a. Create, review and respond to LARs in relation to shipboard installations and system configuration updates. Duties include:
        i. initiating LARs to request the Planning Yard to develop Ship Installation Drawings;
        ii. Review LARs from the Planning Yard requesting system information for interfacing alterations and responding accordingly.

5.3.3.3 Ship Change Documents

5.3.3.4 Assist with the development and review of Ship Change Documents in relation to shipboard alterations and upgrades.

5.3.3.5 Evaluate Maintenance Procedures and Manning Requirements

5.3.3.6 Perform surveys and engineering investigations to evaluate maintenance procedures and manning requirements associated with shipboard equipment and systems. Duties include reviewing the documentation for technical and programmatic accuracy, confirming the recommended fielding plan supports the most current ship availability schedule and ensuring the Cost Benefit Analysis correlates to the cost estimate.

5.4 QUALITY ASSURANCE SUPPORT

The contractor shall generate documentation required to meet RMF requirements, submit required documentation to the relevant Designated Navy Validator / IAM in support to gain ATO.

5.4.1 **Generate the Assess & Authorize (A&A) Plan** – develop documents for the RMF documentation packages that meet all DoD / DISA / DoN requirements tailored to a specific associated system. This includes all supporting RMF documentation such as contingency plan, incident response plan, IAVM plan, combine all artifacts and prepare/deliver project management documents for supporting project with timelines and POAMs. Generate RMF components and artifacts required for the various aspects of the A&A process. These components include, but are not limited to, RMF Implementation Plans, System Identification Plan (SIP), drawings, and POA&M. (CRDL A004)

5.4.2 **Support Program activities** in the form of milestone and issues tracking, document scanning, web site content management, program review session scheduling, and status submittals.

5.4.3 **Services and support assistance** that includes the establishment of Dept-level performance metrics so as to assess the health of programmatic and business aspects, and facilitation of strategic planning sessions.

5.4.4 **Administrative services and support assistance**, to include facilitation of media destruction; coordination/planning for meetings and conferences; preparation and submittal of contractor monthly status, incurred cost, and burn rate analysis reports in addition to monthly invoices.

5.4.5 **Graphic design support and create visual solutions** to communicate messages through print and electronic media including illustration, photography, and various print layout techniques to relay explanation of capabilities, knowledge areas, work areas, and major programs and efforts. 3-D Graphics modeling is a requirement. All graphics support will be provided in Philadelphia for use throughout all NSWCPD locations.

5.4.6 **Presentation materials** Develop booklets, power point presentations, agenda lists, speaker bio lists, upcoming meetings, conference notifications, brochure handouts of presentation, folders, tri-fold brochures, contact list wallet cards, posters, banners, building signage, symposium displays, logo design, information/letterhead development, flyers and invitations. Support includes creation and layout of manuals, annual reports, newsletters, catalogs, video brochures, and videos on DVD and packaging of DVD/CD-Rom. Conduct website design to include concept develop and layout of graphics on website, electronic newsletters. Construct signage and exhibit displays, posters for meetings, conference rooms, testing areas, and indoor/outdoor events such as in service day. Meeting kiosks with instructional videos. Develop test site materials including instructional videos, booklets, signs, DVD/CD-Rom, and brochures describing equipment on test sites, and information on explaining the purpose of the equipment and how the equipment is used.

5.4.7 **Configuration Management** of system related software products, requirements documentation and interface specifications. Provide requirements traceability support through test procedures and ensure records are kept accordingly. The Contractor shall participate in and conduct audit procedures to validate proper systems engineering policies are followed. Procedures shall be documented in accordance with CDRL A006. Perform identification, condition assessments, and labeling in accordance with NAVSEA Standard Items. Provide Quality Assurance and inspection support for the proper installation of technologies being introduced into existing platforms. Support system accreditation activities and deliver documentation in accordance with CDRL A012. Work as part of a project team to coordinate database development and determine project scope and limitations. Select and enter codes to monitor database performance and to create production database. Identify and evaluate industry trends in database systems to serve as a source of information and advice for upper management. Review workflow charts developed by programmer analyst to understand tasks computer will perform, such as updating re

cords. Contractor shall provide Navy Information Dominance Approval System (NAVIDAS) IT Support including reviewing and approving NAVIDAS purchase requests against DoN Policy and requirements; update NAVIDAS checklists and guidebook to assist Philadelphia users in creating IT purchase requests.

5.4.8 Financial Analysis and Management and Preparation of Presentation Materials. Effort is in support of RMF to ensure all requirements are followed throughout RMF life cycle. Briefs are conducted on a weekly basics to updated program offices and leadership. Multiple levels of resources are pulled together to provide a clear status of all efforts tied together with RMF & Cyber Security. Cyber Hygiene is key for compliance. Cyber Security workforce resources need to follow strict guidelines which is an audit point conducted by cyber security resources.

5.4.8.1 Contractor shall provide on-site administrative services and support assistance including word processing, copy and file letters, reports, memos, and other similar types of documents.

5.4.8.2 Maintain currency of correspondence procedures in accordance with our local instructions. All correspondence shall be proofread, edited, and corrected for errors in format and grammar.

5.4.8.3 Contractor shall maintain master project calendar and coordinating arrangements for presentation/meetings.; record time and attendance using ERP; entering purchase requests into ERP (excluding contracts PRs and PRs specifically for the Contractor); help support network account information on System Access Authorization Request (SAAR) forms. Also enter data into various computerized databases and tracking systems and create spreadsheets and graphs based on the information contained in these systems; and manage office supplies.

5.4.8.4 Maintain hard copies of direction, instructions, and other documents that are required to support documentation audits.

5.4.8.5 Contractor shall assist with NSWCPD security badge information entry and security badge documentation processing.

5.4.8.6 Contractor shall provide on-site administration services to process and track badge and swipe card services and support assistance requests in accordance with our Division instructions and procedures.

5.5 ASSESS & AUTHORIZE/RISK MANAGEMENT FRAMEWORK PACKAGE PREPARATION AND DOCUMENTATION

5.5.1 This requirement calls for the preparation and submission of approximately 74 + total A&A Packages for ATO. There are three levels of complexity – Small, Medium, and Large. Small packages are typically comprised of 1-6 assets, Medium packages are typically comprised of 7-12 assets, and large packages are typically comprised of 13 or more assets, and contain a mix of workstations and servers.

5.5.2 Develop RMF A&A package documentation required for ATO-submission in accordance with DoD/NAVSEA directives, which includes the following components: Platform IT (PIT) Determination package documentation, System Categorization Form, Information System Continuous Monitoring Strategy (ISCM), Security Plan (SP), Step Concurrence forms, Plan of Actions and Milestones (POA&M), Security Assessment Plan (SAP), Security Assessment Report (SAR), Risk Assessment Report (RAR), Security Authorization Package, CYBERSAFE Certification, Package Endorsement Letters

5.5.3 Ensure RMF A&A package is submitted to the Certification Authority (CA) in sufficient time for its review and operational cybersecurity risk recommendation to obtain Designated Accrediting Authority (DAA) authorization decision; authorization must be obtained prior to operations or tests on a live network (i.e. LBES or shipboard).

5.5.4 Follow the published Navy, NAVSEA Business Rules (i.e. ODAA, Authorizing Official Designated Representative (AODR), and PIT Validation guidance when preparing C&A/A&A packages; should there be any conflicting interpretations, request for clarification/adjudication will be resolved by the Government Information Assurance Manager (IAM)/Information System Security Manager (ISSM).

5.5.5 Coordinate with the government-appointed Navy Validator throughout the C&A/A&A package creation and processing to ensure compliance with stated regulations to help ensure an efficient package-submission that results in ATO; Contractor shall inform the Navy Validator when artifacts are produced; Contractor shall submit completed C&A/A&A Packages to the government-appointed Navy Validator for validation of C&A/A&A Packages

5.5.6 **Documentation** Develop and maintain a Plan of Action and Milestone (POA&M) for all IA-related tasks and deliverables in accordance with the Security Technical

Implementation Guide (STIG); Information shall be delivered in accordance with, and report on project goals and objectives, work breakdown structure, description of milestones and deliverables, schedule for deliverables including interim and formal reviews, and project risks and mitigation strategies. Develop Risk Assessment Reports (RARs) based on vulnerability test results, automated scan reviews, Assured Compliance Assessment Solution (ACAS) scans, and other DoD-mandated assessment-utilities. Reports shall be delivered in accordance with CDRL A010 and follow DISA Security Technical Implementation Guides (STIGs). Document C&A/A&A-information in the C&A/A&A Package consistent with all other Packages, and ensure that there are no omissions. Input reports in eMASS, or deliver in MS Office-products/Visio formats, as appropriate; activity shall be noted in accordance with; Contractor may require access to both classified and unclassified eMASS.

5.6 CERTIFICATION TEST AND EVALUATION

5.6.1 Develop and test new security features to be implemented into the Control System Operating Environment; run tests on the hardware and/or software to help determine the effectiveness of the newly developed security features; the developed security features shall be delivered in accordance with.

5.6.2 Monitor and maintain the security posture of IT systems in accordance with each systems SOP; tasks include patching, implementing STIGs, analyzing network traffic, and applying new physical security measures

5.6.3 Ensure system's compliance with all applicable Information Assurance Controls (IACs) for an assigned DON system within the NAVSEAINST 9400.2 guidelines; tasks include the development of the appropriate test procedures, if necessary, and the test procedure shall be delivered; execution of the test procedures; and documentation of the results of security testing.

5.6.4 Review CT&E test plans and procedures to ensure the test plan(s) are comprehensive enough to addresses the corresponding level of effort, and will validate all IA requirements applicable to the IT system or Site being certified and accredited; findings shall be reported in accordance with.

5.7 C&A PACKAGE ASSESSMENT SUPPORT

5.7.1 Register and be listed on the official list of Navy Qualified Validators; perform and support activities of Validators of Navy (RMF) Risk Management Framework packages.

5.7.2 Perform as an independent third party who assesses and validates that the system has [or has not] implemented the approved security control baseline. The Validator acts as a trusted agent to the (SCA) Security Control Assessor and SCA Liaison. Assessments shall be delivered~~ in accordance with CDRL A011~~.

5.7.3 Optimize C&A test and validation procedures to ensure the most accurate reporting; Contractor shall ensure findings are presented in the appropriate format (9400.2M) and that all IA requirements have been addressed.

5.8 VALIDATION DOCUMENTATION SUPPORT

5.8.1 Requirement calls for the review and validation of the (RMF) Risk Management Framework Packages for ATO submitted as required of Section 5.7 of this SOW. NSWCPD abides by the Navy Certification Agent Qualification Standards and Registration Guidebook when performing validation activities. In addition to DIACAP C&A requirements and the DoD Instruction 8510.01, Subj: Risk Management Framework (RMF) for DoD Information Technology (IT) also takes effect per NAVSEA guidance. Certification & Accreditation (C&A) Validation must be in accordance with NAVSEAINST 9400.2, which comprises the activities required for (C&A). Validation including associated supporting documentation such as validation test procedures, validation artifacts, validation plans and procedures, compliance status, validation tests, validation results/reports. CDRL A012

5.8.2 **Verification/Assessment**
Register and be listed on the official list of Navy Qualified Validators; perform and support activities of Validators of Navy (RMF) Risk Management Framework packages.

5.8.3 **Validate**
Perform as an independent third party who assesses and validates that the system has [or has not] implemented the approved security control baseline. The Validator acts as a trusted agent to the (SCA) Security Control Assessor and SCA Liaison. Ensure separation of duties between ISSM and (NQV).

5.8.4 **Preparation**
Prepare the Security Assessment Plan (SAP) with input from the system's ISSE and ISSM. The SAP is to submitted and approved by the SCA in accordance (NAVSEAINST 9400.2) instruction. Ensure separation of duties between ISSM and (NQV).

5.9 REMEDIATION

5.9.1 Evaluate all discrepancies reported by Validators, and recommend mitigation measures for reducing or eliminating specific risk items; recommendations shall be reported in accordance with CDRL A010.

5.9.2 Address deficiencies reported by from Validators by executing approved-remediation methods to harden and secure the system; work includes STIGs, patching, scanning, validation of inventory and creation of network diagrams.

5.9.3 Coordinate with the ISSE/ISO-equivalent to NSWCPD's Information Assurance Officer (IAO) to determine and fix [and/or mitigate] identified weaknesses, and to determine the level of revalidation testing required should immediate fixes not be applied

5.9.4 Provide by in-person, phone or e-mail support as appropriate to respond to Validator requests; all requests/inquiries shall be addressed within one business day.

5.10COMPLIANCE REPORTING SUPPORT

5.10.1 Document

Utilize the Security Assessment Report (SAR) to document the residual risk of the non-compliant security controls remaining after the risk assessment work is complete; documentation of the residual risk shall be in the Risk Assessment Report (RAR) in accordance (NAVSEAINST 9400.2) instruction.

5.10.2 Ensure system's compliance

Ensure each element of the enclave will provide a RAR with input from a Level II Validator, as defined in Qualification Standards, Responsibilities, and Registration Process for Navy Qualified Validator (NQV) in accordance (NAVSEAINST 9400.2) instruction.

5.10.3 Optimize

Contractor (NQV) independent element-level RAR shall feed into the enclave-level RAR. The enclave-level RAR will be signed/endorsed by a Level III Validator.

6.0 DATA REQUIREMENTS

All Contracts Data Requirements Lists (CDRL) shall reflect both prime and subcontractor data if applicable at the same level of detail. CDRLs shall be delivered electronically, unless otherwise stated, and while Contractor's format is acceptable, Government's approval is required from the COR.

- Contract Status Report (CDRL A001)
- Travel Report (CDRL A002)
- Contractor's Personnel Roster (CDRL A003)
- Plan of Action and Milestone (POA&M) Schedule (CDRL A004)
- Quality Assurance (QA) Workbook (CDRL A005)
- In-Process Control Procedures (IPCPs) (CDRL A006)
- Weekly Production Status Reports (CDRL A007)
- Lessons-Learned Report (CDRL A008)
- Minutes of Meetings (CDRL A009)
- Database or other Electronic Documents (CDRL A010)
- System Accreditation Documentation (CDRL A012)
- CSWF Training and Certification (CDRL A013)
- Technical Report Study/Services (CDRL A014)
- Government Property Inventory Report (CDRL A015)
- Systems Security Plan (CDRL A016)

7.0 SECURITY REQUIREMENTS

An active **SECRET** Facility Clearance (FLC) is required for performance on this contract. There is no safeguarding requirement required. All personnel must have a current **SECRET** or higher clearance, or the ability to obtain one.

7.1 **SECURITY TRAINING:** The Contractor is responsible for completing all required Government mandated training to maintain security and network access to government sites and IT systems. Training requirements include but are not limited to: Antiterrorism Level 1 Awareness; DoD Cyber Awareness Challenge; Combatting Human Trafficking; Records Management in the DON: Everyone's Responsibility; Training and Readiness: The Active Shooter; Constitution Day; NAVSEA Introduction to Controlled Unclassified Information; Operations Security (OPSEC); NAVSEA Counterintelligence Training; Privacy and Personally Identifiable Information (PII) Awareness Training; and NAVSEA Physical Security training. Certificates of successful completion shall be sent to the COR and as otherwise specified in the contract. Certificates of successful completion shall be sent to the COR and as otherwise specified in the contract.

7.2 In accordance with SECNAV M-5510.30 Chapters 5 and 6, all Contractor personnel that require access to Department of Navy (DON) information systems and/or work on-site are designated Non-Critical Sensitive/IT-II positions, which require an open investigation or favorable adjudicated National Agency Check (NACLC) by the Industrial Security Clearance Office (DISCO). Investigations should be completed using the SF-86 Form and the SF-87 finger print card. An interim clearance can be granted by the company Security Officer and recorded in the Joint Personnel Adjudication System (JPAS). An open or closed investigation with a favorable adjudication is required prior to issuance of a badge providing access to NSWCPD sites and buildings. If an unfavorable adjudication is determined by DCSA all access will terminated. For Common Access Card (CAC) card you must have a completed investigation that has been favorably adjudicated or a final security clearance. A CAC Card will not be issued to contractors who have an interim security clearance.

7.3 **ON SITE WORK:** Contractor personnel that require a badge to work on-site at one of the NSWCPD sites must provide an I-9 form to verify proof of citizenship. The I-9 form should be signed by the company Facility Security Officer or the company Human Resource Department. In addition to the I-9 form, Contractors shall also bring their birth certificate, current United States Passport or naturalization certificate and state issued ID to the NSWCPD Security Officer at the time of badge request to verify citizenship. Finally, contractors shall supply a copy of their OPSEC Training Certificate or other proof that the training has been completed.

7.4 In accordance with NSWCPD security protocol, contractor employees who hold dual citizenship will not be granted security clearance to our facilities.

7.5 A Facility Access Determination (FAD) will be completed on any contractor that does not have a favorable adjudicated investigation in JPAS and is requesting swipe/non-swipe access to our buildings in excess of 120 days. Any contractor that has unfavorable information that has not been favorably adjudicated by Department of Defense Central Adjudication Facility (DOD CAF) will not be issued a badge.

7.6 **DD254 REQUIREMENT:** This effort may require access to classified information up to the **SECRET** level. No classified data will be generated or stored by the Contractor. The Contractor is required to have and maintain a SECRET clearance. The requirements of the attached DD Form 254 apply.

7.7 The contract company shall ensure each employee has completed the 10-hour OSHA Maritime Shipyard Employment Course #7615. The contract company shall ensure that each employee maintains a current Course #7615 certification based on the course's certification expiration period and the requirement for retraining and recertification. REF: NAVSEA SI 009-74

7.8 The Contractor shall appoint a Facility Security Officer (FSO), who shall (1) be responsible for all security aspects of the work performed under this contract, (2) assure compliance with the National Industrial Security Program Operating Manual (NISPOM) (DOD 5220.22-M), and (3) assure compliance with any written instructions from the NSWCPD, Security Office Dorothy Morton.

7.9 The Prime Contractor shall:

7.9.1 Forward signed copies of DD254s provided to subcontractors to the Naval Surface Warfare Center Philadelphia Division (NSWCPD), ATTN: Security.

7.9.2 Direct the subcontractor to obtain approval, through the prime Contractor, for the public release of information received or generated by the sub through the prime Contractor.

7.9.3 Submit the subcontractor request for public release through the technical point of contact identified on the DD 254.

7.10All Contractor-personnel accessing classified information or material associated with and/or performing work relative to the resultant contract must be United States citizens and shall have and maintain at a minimum a final SECRET security clearance at time of contract award. Certain personnel designated by the Program Manager will be required to have and maintain at a minimum a final SECRET security clearance.

7.11Contractor requires access to Restricted Data (RD) information in performance on this contract to support efforts that are related to nuclear propulsion plants. This access is required to access the secure spaces ships and certain land based test facilities. Access is required to obtain and review the associated logistical and system related documentation.

7.12Contractor requires access to Non-SCI information in performance on these contract support efforts that are related to nuclear propulsion plants. This access is required to access the secure spaces ships and certain land based test facilities. Access is required to obtain and review the associated logistical and system related documentation.

7.13Contractor requires access to NNPI information in performance on this contract to support efforts that are related to nuclear propulsion plants. This access is required to access the secure spaces ships and certain land based test facilities. Access is required to obtain and review the associated logistical and system related documentation.

7.14Security Classification Guidance is as follows of portions of the tasking on this contract when invoked in the task order statement of work:

7.15Contractor requires access to information and equipment classified at the Confidential National Security Information (NSI) level in order to provide industrial support services within facilities that actively supports the Navy Nuclear Propulsion Program (NNPP).

7.16All contractor personnel accessing classified information or classified material associated with the performance work relative to the resultant contract must be United States citizens no foreign nationals and shall have and maintain at a minimum Confidential security clearance.

7.17The Contractor is responsible for completing all required government mandated training to maintain security and network access to government sites and IT systems, as necessary to support.

Additional information related to the facility clearance process can be obtained by visiting www.dss.mil or http://www.dss.mil/isec/pcl_index.htm.

7.18The planned utilization of non-U.S. Citizens in the performance of this contract effort must be identified by name and country of citizenship in the proposal. Foreign Nationals shall not be allowed access to classified or critical program information unless approved on a case by case basis by DSS.

8.0 Planning, Programming, Budgeting and Execution (PPBE) Data.

When contractor employees, in the performance of their duties, are exposed to Planning, Programming, Budgeting and Execution (PPBE) data, a Non-Disclosure Agreement (NDA) with all affected contactor personnel must be executed in coordination with the COR and PCO to ensure safeguarding disclosure of this data.

9.0 Safeguarding Covered Defense Information and Cyber Incident Reporting

9.1 System Security Plan and Plans of Action and Milestones (SSP/POAM) Reviews

9.1.1 Within thirty (30) days of contract award, the Contractor shall make its System Security Plan(s) (SSP(s)) for its covered contractor information system(s) available for review by the Government at the contractor's facility. The SSP(s) shall implement the security requirements in Defense Federal Acquisition Regulation Supplement (DFARS) clause

252.204-7012, which is included in this contract. The Contractor shall fully cooperate in the Government's review of the SSPs at the Contractor's facility.

9.1.2 If the Government determines that the SSP(s) does not adequately implement the requirements of DFARS clause 252.204-7012 then the Government shall notify the Contractor of each identified deficiency. The Contractor shall correct any identified deficiencies within thirty (30) days of notification by the Government. The contracting officer may provide for a correction period longer than thirty (30) days and, in such a case, may require the Contractor to submit a plan of action and milestones (POAM) for the correction of the identified deficiencies. The Contractor shall immediately notify the contracting officer of any failure or anticipated failure to meet a milestone in such a POAM.

9.1.3 Upon the conclusion of the correction period, the Government may conduct a follow-on review of the SSP(s) at the Contractor's facilities. The Government may continue to conduct follow-on reviews until the Government determines that the Contractor has corrected all identified deficiencies in the SSP(s).

9.1.4 The Government may, in its sole discretion, conduct subsequent reviews at the Contractor's site to verify the information in the SSP(s). The Government will conduct such reviews at least every three (3) years (measured from the date of contract award) and may conduct such reviews at any time upon thirty (30) days' notice to the Contractor.

9.2 <u>Compliance to NIST 800-171</u>

9.2.1 The Contractor shall fully implement the CUI Security Requirements (Requirements) and associated Relevant Security Controls (Controls) in NIST Special Publication 800-171 (Rev. 1) (NIST SP 800-171), or establish a SSP(s) and POA&Ms that varies from NIST 800-171 only in accordance with DFARS clause 252.204-7012(b)(2), for all covered contractor information systems affecting this contract.

9.2.2 Notwithstanding the allowance for such variation, the contractor shall identify in any SSP and POA&M their plans to implement the following, at a minimum:

9.2.2.1 Implement Control 3.5.3 (Multi-factor authentication). This means that multi-factor authentication is required for all users, privileged and unprivileged accounts that log into a network. In other words, any system that is not standalone should be required to utilize acceptable multi-factor authentication. For legacy systems and systems that cannot support this requirement, such as CNC equipment, etc., a combination of physical and logical protections acceptable to the Government may be substituted;

9.2.2.2 Implement Control 3.1.5 (least privilege) and associated Controls, and identify practices that the contractor implements to restrict the unnecessary sharing with, or flow of, covered defense information to its subcontractors, suppliers, or vendors based on need-to-know principles;

9.2.2.3 Implement Control 3.1.12 (monitoring and control remote access sessions) - Require monitoring and controlling of remote access sessions and include mechanisms to audit the sessions and methods.

9.2.2.3.1 Audit user privileges on at least an annual basis;

9.2.2.3.2 Implement:

9.2.2.3.2.1 Control 3.13.11 (FIPS 140-2 validated cryptology or implementation of NSA or NIST approved algorithms (i.e. FIPS 140-2 Annex A: AES or Triple DES) or compensating controls as documented in a SSP and POAM); and,

9.2.2.3.2.2 NIST Cryptographic Algorithm Validation Program (CAVP) (see https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program);

9.2.2.3.2.3 Implement Control 3.13.16 (Protect the confidentiality of CUI at rest) or provide a POAM for implementation which shall be evaluated by the Navy for risk acceptance.

9.2.2.3.2.4 Implement Control 3.1.19 (encrypt CUI on mobile devices) or provide a plan of action for implementation which can be evaluated by the Government Program Manager for risk to the program.

9.3 **Cyber Incident Response:**

9.3.1 The Contractor shall, within fifteen (15) days of discovering the cyber incident (inclusive of the 72-hour reporting period), deliver all data used in performance of the contract that the Contractor determines is impacted by the incident and begin assessment of potential warfighter/program impact.

9.3.2 Incident data shall be delivered in accordance with the Department of Defense Cyber Crimes Center (DC3) Instructions for Submitting Media available at http://www.acq.osd.mil/dpap/dars/pgi/docs/Instructions_for_Submitting_Media.docx. In delivery of the incident data, the Contractor shall, to the extent practical, remove contractor-owned information from Government covered defense information.

9.3.3 If the Contractor subsequently identifies any such data not previously delivered to DC3, then the Contractor shall immediately notify the contracting officer in writing and shall deliver the incident data within ten (10) days of identification. In such a case, the Contractor may request a delivery date later than ten (10) days after identification. The contracting officer will approve or disapprove the request after coordination with DC3.

9.4 **Naval Criminal Investigative Service (NCIS) Outreach**

9.4.1 The Contractor shall engage with NCIS industry outreach efforts and consider recommendations for hardening of covered contractor information systems affecting DON programs and technologies.

9.5 **NCIS/Industry Monitoring**

9.5.1 In the event of a cyber incident or at any time the Government has indication of a vulnerability or potential vulnerability, the Contractor shall cooperate with the Naval Criminal Investigative Service (NCIS), which may include cooperation related to: threat indicators; pre-determined incident information derived from the Contractor's infrastructure systems; and the continuous provision of all Contractor, subcontractor or vendor logs that show network activity, including any additional logs the contractor, subcontractor or vendor agrees to initiate as a result of the cyber incident or notice of actual or potential vulnerability.

9.5.2 If the Government determines that the collection of all logs does not adequately protect its interests, the Contractor and NCIS will work together to implement additional measures, which may include allowing the installation of an appropriate network device that is owned and maintained by NCIS, on the Contractor's information systems or information technology assets. The specific details (e.g., type of device, type of data gathered, monitoring period) regarding the installation of an NCIS network device shall be the subject of a separate agreement negotiated between NCIS and the Contractor. In the alternative, the Contractor may install network sensor capabilities or a network monitoring service, either of which must be reviewed for acceptability by NCIS. Use of this alternative approach shall also be the subject of a separate agreement negotiated between NCIS and the Contractor.

9.5.3 In all cases, the collection or provision of data and any activities associated with this statement of work shall be in accordance with federal, state, and non-US law.

10.0U-NNPI SECURITY REQUIREMENTS

10.1Security Classification Guidance is as follows of portions of the tasking on this contract when invoked in the task order statement of work:

10.1.1 Contractor requires access to information and equipment classified at the Confidential National Security Information (NSI) level in order to provide industrial support services within facilities that actively supports the Navy Nuclear Propulsion Program (NNPP).

10.1.2 All contractor personnel accessing classified information or classified material associated with the performance work relative to the resultant contract must be United States citizens no foreign nationals and shall have and maintain at a minimum Confidential security clearance.

10.1.3 The Contractor is responsible for completing all required government mandated training to maintain security and network access to government sites and IT systems, as necessary to support.

10.1.4 **U-NNPI**

10.1.4.1 Purpose. The Contractor hereby agrees that when provided documents (specifications, drawings, etc.) that are marked as containing NOFORN sensitive information that must be controlled pursuant to Federal law, the information contained therein and generated as part of the inquiry shall be used only for the purpose stated in the contract and shall in no case be transmitted outside the company (unless such transmittals comply with the detailed guidance of the contract) or to any foreign national within the company. While in use, the documents shall be protected from unauthorized observation and shall be kept secure so as to preclude access by anyone not having a legitimate need to view them. The documents shall not be copied unless done in conformance with the detailed guidance of the contract. All the documents shall be promptly returned in their entirety, unless authorized for proper disposal or retention, following completion of the contract.

10.1.4.2 Specific Requirements for Protecting U-NNPI

a) Only U.S. citizens who have an NTK required to execute the contract shall be allowed access to U-NNPI.
b) When not in direct control of an authorized individual, U-NNPI must be secured in a locked container (e.g., file cabinet, desk, safe). Access to the container must be such that only authorized persons can access it, and

compromise of the container would be obvious at sight. Containers should have no labels that indicate the contents. If removed from the site, U-NNPI must remain in the personal possession of the individual. At no time should U-NNPI be left unsecured (e.g., in a home or automobile, or unattended in a motel room or sent with baggage).

c) U-NNPI documents will have the word NOFORN at the top and bottom of each page. The cover sheet will have the warning statement shown below. Documents originated in the course of work that reproduce, expand or modify marked information shall be marked and controlled in the same way as the original. Media such as video tapes, disks, etc., must be marked and controlled similar to the markings on the original information.

d) U-NNPI may not be processed on networked computers with outside access unless approved by CNO (N00N). If desired, the company may submit a proposal for processing NNPI on company computer systems. Personally owned computing systems, such as personal computers, laptops, personal digital assistants, and other portable electronic devices are not authorized for processing NNPI. Exceptions require the specific approval of the cognizant DAA and CNO (N00N).

e) U-NNPI may be faxed within the continental United States and Hawaii provided there is an authorized individual waiting to receive the document and properly control it. U-NNPI may not be faxed to facilities outside the continental United States, including military installations, unless encrypted by means approved by CNO (N00N).

f) U-NNPI may be sent within the continental United States and Hawaii via first class mail in a single opaque envelope that has no markings indicating the nature of the contents.

g) Documents containing U-NNPI shall be disposed of as classified material.

h) Report any attempts to elicit U-NNPI by unauthorized persons to the appropriate security personnel.

i) Report any compromises of U-NNPI to the appropriate security personnel. This includes intentional or unintentional public release via such methods as theft, improper disposal (e.g., material not shredded, disks lost), placement on Web site, transmission via email, or violation of the information system containing U-NNPI.

j) The only approved storage for U-NNPI is CDMS NOFORN.

11.0PLACE OF PERFORMANCE

11.1The primary place of performance shall be at NSWCPD in Philadelphia or the contractor facility. The individual technical instruction for the task shall dictate the location. Travel may be required to the locations listed in Section 12.

11.2In addition, this Task Order may require on-site support at the following fleet concentration locations: Naval Station Norfolk, Norfolk, VA; Naval Station Mayport, Jacksonville, FL; Naval Station San Diego, San Diego, CA; Joint Base Pearl Harbor – Hickam, Pearl Harbor, HI, Ship Repair Facility Japan – Yokosuka, Japan

11.3Performance will occur at the following government sites: NSWCPD, Naval Station Norfolk, Naval Station Mayport, Naval Station San Diego, Naval Station Everett, Washington Navy Yard, Joint Base Pearl Harbor, Ship Repair Facility Japan, Naval Support Activity Sasebo, Naval Support Activity Rota, Naval Support Activity Naples, and Naval Support Activity Bahrain.

11.4Government will provide kiosk workstation, NMCI & RDT&E asset, if required, printer and phone, space for up to (30) Contractor personnel under this task order.

11.5The specific location(s) will be provided at time of award of the Task Order. The Contractor shall provide a list of employees who require access to these areas, including standard security clearance information for each person, to the Contracting Officer Representative (COR) no later than three business days after the date of award. The work space provided to the Contractor personnel shall be identified by the Awardee, with appropriate signage listing the company name and individual Contractor employee name.

11.6Access to Government buildings at Naval Surface Warfare Center Philadelphia Division is from 0600 to 1800 Monday through Friday, except Federal holidays. Normal work hours are from 0600 to 1800, Monday through Friday. Contractor employees shall be under Government oversight at all times. Government oversight requires that a Government employee be present in the same building/facility whenever Contractor employee(s) are performing work under this Task Order. Contractor personnel are not allowed to access any Government buildings at NSWCPD outside the hours of 0600 to 1800 without the express approval of the Procuring Contracting Officer (PCO).

11.6.1 Early Dismissal and Closure of Government Facilities

11.6.1.1 When a Government facility is closed and/or early dismissal of Federal employees is directed due to severe weather, security threat, or a facility related problem that prevents personnel from working, onsite Contractor personnel regularly assigned to work at that facility should follow the same reporting and/or departure directions given to Government personnel. The Contractor shall not direct charge to the contract for time off, but shall follow its own company policies regarding leave. Non-essential Contractor personnel, who are not required to remain at or report to the facility, shall follow their parent company policy regarding whether they should go/stay home or report to another company facility. Subsequent to an early dismissal and during periods of inclement weather, onsite Contractors should monitor radio and television announcements before departing for work to determine if the facility is closed or operating on a delayed arrival basis.

11.6.1.2 When Federal employees are excused from work due to a holiday or a special event (that is unrelated to severe weather, a security threat, or a facility related problem), on site Contractors will continue working established work hours or take leave in accordance with parent company policy. Those Contractors who take leave shall not direct charge the non-working hours to the Task Order. Contractors are responsible for predetermining and disclosing their charging practices for early dismissal, delayed openings, and closings in accordance with the FAR, applicable cost accounting standards, and company policy. Contractors shall follow their disclosed charging practices during the Task Order period of performance, and shall not follow any verbal directions to the contrary. The PCO will make the determination of cost allowability for time lost due to facility closure in accordance with FAR, applicable Cost Accounting Standards, and the Contractor's established accounting policy.

11.6.2 The contractor shall ensure that each contractor employee who will be resident at NSWCPD completes the Environmental Management System (EMS) Awareness training within 30 days of commencing performance at NSWCPD. This document is available at: https://navsea.navy.deps.mil/wc/pnbc-code10/Safety/default.aspx

11.6.3 In accordance with C-223-W002, ON-SITE SAFETY REQUIREMENTS (NAVSEA), the contractor shall certify by e-mail to Paul Breeden (paul.breeden@navy.mil) that on-site employees have read the "Philadelphia Division Environmental Policy and Commitment" and taken the EMS Awareness training within 30 days of commencing performance at NSWCPD. The e-mail shall include the employee name, work site, and contract number.

12.0TRAVEL

12.1The Contractor may be required to travel from the primary performance location when supporting this requirement. The estimated number of trips is **30 per year**. Travel in support of this requirement is anticipated to include, but may not be limited to, the following alternate performance locations:

At Sea: The Contractor may be required to support test events and fleet technical assists underway onboard a Navy vessel.

CONUS/OCONUS	DESTINATION	Estimated Number of Trips	Number of People	Number of Days Per Trip
CONUS	Naval Station, Norfolk, VA	1	2	5
CONUS	NSWC Philadelpiha, Phiadelphia, PA	12	2	5
CONUS	Naval Station, Mayport, FL	2	2	5
CONUS	Naval Station, San Diego, CA	2	2	5
CONUS	Naval Base, Coronado, CA	1	2	5

CONUS	Puget Sound Naval Shipyard & Intermediate Maintenance Facility (PSNS&IMF), Bremerton, WA	1	2	5
CONUS	Naval Station Everett, WA	2	2	5
CONUS	Washington, DC	2	2	5
CONUS	Charlottesville, VA	2	2	5
CONUS	NSWC Dahlgren, Dahlgren, VA	2	2	5
CONUS	Hunington Beach, CA	1	2	5
CONUS	Orlando, Florida	2	2	5
CONUS	HII Pascagoula, Mississippi	2	2	5
CONUS	BIW Shipyard/SUPSHIP, Bath, Maine	2	2	5
CONUS	Kitsap, WA	1	2	5
CONUS	Charlottesville, SC	4	2	5
CONUS	Portsmith, VA	2	2	5
CONUS	Norfolk, VA	3	2	5
CONUS	Massachusetts, ME	2	2	5
CONUS	Pascagoula, MS	2	2	5
CONUS	Road Island, ME	2	2	5
CONUS	Panama City, FL	2	2	5
CONUS	Mayport, FL	2	2	5
CONUS	New Orleans, Lousiana	2	2	5
CONUS	Austal Shipyard, Mobile, AL	2	2	5
CONUS	Marinette Shipyard, Marinette, WI	1	2	5
CONUS	Naval Station Great Lakes, IL	1	2	5
OCONUS	Ship Repair Facility (SRF) and Combined	1	2	5

	Fleet Activities (CFAY), Yokosuka, Japan			
OCONUS	SFF Detachment and Combined Fleet Activities Sasebo (CFAS), Japan	1	2	5
CONUS	Naval Station Pearl Harbor, HI	1	2	5
OCONUS	Naval Station Rota, Spain	1	2	5
OCONUS	Naval Support Activity Naples, Italy	1	2	5
OCONUS	Sembawang Base, Sembawang, Singapore	1	2	5
OCONUS	Hong Kong, China	1	2	5
OCONUS	Busan, South Korea	1	2	5
OCONUS	Naval Support Activity. Manama, Bahrain	1	2	5
OCONUS	Dubai, United Arab Emirates	1	1	5

12.2The number of times the Contractor may be required to travel to each location cited above may vary as program requirements dictate, provided that the total estimated travel cost is not exceeded. The numbers of trips and types of personnel traveling shall be limited to the minimum required to accomplish work requirements. All travel shall be approved by the COR and Contracting Officer before travel occurs. Approval may be via the Technical Instruction (TI). In accordance with the TI instructions, before initiating any travel the Contractor(s) shall submit a detailed and fully-burdened estimate that includes the number of employees traveling, their expected travel costs for airfare, lodging, per diem, rental car, taxi/mileage and any other costs or actions requiring approval. The travel estimate shall be submitted to the Contracting Officer's Representative (COR) and Contract Specialist. Actuals cost, resulting from the performance of travel requirements, shall be reported as part of the Contractor's monthly status report. The reportable cost shall also be traceable to the Contractor's invoice

12.3All travel shall be conducted in accordance with FAR 31.205-46, Travel Costs, and B-231-H001 Travel Cost (NAVSEA) and shall be pre-approved by the COR. The Contractor shall submit travel reports in accordance with DI-MGMT-81943 (CDRL A002).

12.4**Travel Costs**

12.4.1 The current "maximum per diem" rates are set forth in the (i) Federal Travel Regulations for travel in the Continental United States; (ii) Joint Travel Regulations for Overseas Non-Foreign areas (e.g., Alaska, Hawaii, Guam, Puerto Rico, etc.); and (ii) Department of State (DOS) prescribed rates for foreign overseas locations.

13.0GOVERNMENT FURNISHED PROPERTY

The Government intends to provide all GFP identified in Attachment E in Section J is anticipated to be provided within 90-days after clearance verification.

The Contractor shall be required to acquire Privilege User Access Authority (PAA) respective of the Windows 2000/XP/7/10 & Linux Operating System and beyond in accordance with Section 12.2 " Navy Information Assurance (IA) Workforce Requirements".

14.0GOVERNMENT FURNISHED INFORMATION

The Government will provide access to NIPR and SIPRNET networks associated to all relevant government information to meet the required work effort.

GFI is for informational purposes and that use by the Contractor is optional.

15.0PURCHASES

15.1Only items directly used and incidental to the services for this Task Order and for work within the scope of the SOW, shall be purchased under the Other Direct Cost (ODC) line items. Individual purchases above $10,000 shall be approved by the Contracting Officer prior to purchase by the Contractor. The purchase request and supporting documentation shall be submitted via email to the Contracting Officer and the Contracting Officer's Representative (COR) it shall be itemized and contain the cost or price analysis performed by the Contractor to determine the reasonableness of the pricing. Provide copies of price estimates from at least two (2) vendors.

15.2Information Technology (IT) equipment, or services must be approved by the proper approval authority. All IT requirements, regardless of dollar amount, submitted under this Contract/Task Order shall be submitted to the PCO for review and approval prior to purchase. The definition of information technology is identical to that of the Clinger-Cohen Act, that is, any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

16.0PERSONNEL

Personnel Requirements. All persons proposed in key and non-key labor categories shall, at the time of proposal submission, be U.S. citizens holding at least a current **SECRET** clearance, or possess a favorable DCSA adjudication as outlined in Section 11 of this SOW.

Clause 52.222-2 "Payment for Overtime Premiums" will provide for the total approved dollar amount of overtime premium or will state “zero” if not approved. If overtime premium has not been approved under this contract in accordance with Clause 52.222-2, overtime effort to be performed shall be requested from the Contracting Officer prior to performance of premium overtime. For overtime premium costs to be allowable costs; the Contracting Officer is required to approve the performance of overtime prior to the actual performance of overtime. The dollar amount in FAR 52.222-2 shall equal overtime premium negotiated between the Government and the prime contractor. This overtime premium amount shall equal the prime contractor's unburdened premium OT labor costs plus the subcontractors' fully burdened premium OT labor costs.

The level of effort for the performance of the resultant Task Order is based on the following labor categories and hours:

Title	eCRAFT Code	Key	Hours	OT Hours	Resumes Req
MANAGER, PROGRAM/PROJECT II	MANP2	Yes	9600	0	1
ANALYST, MANAGEMENT II	ANM2	No	9600	250	0
ENGINEER, COMPUTER II	EC2	No	9600	550	0
ENGINEER, SYSTEMS II	ESY2	No	9600	550	0
ENGINEER, MECHANICAL III	EM3	No	8815	285	0
ENGINEER, DESIGN III	ED3	No	9600	250	0
COMPUTER OPERATOR I	14041	No	9600	550	0
COMPUTER OPERATOR II	14042	No	9600	550	0
COMPUTER OPERATOR III	14043	No	9600	550	0
COMPUTER OPERATOR IV	14044	No	9600	550	0
COMPUTER OPERATOR V	14045	No	9600	550	0
MANAGER, PROGRAM/PROJECT I	MANP1	No	9600	0	0
TECHNICIAN, ENGINEERING II	30082	No	9600	550	0
TECHNICIAN, ENGINEERING III	30083	No	9600	550	0
TECHNICIAN, ENGINEERING IV	30084	No	9600	500	0
ENGINEER, SYSTEMS IV	ESY4	No	8815	285	0
ENGINEER, DESIGN IV	ED4	No	8815	285	0
ENGINEER, ELECTRICAL/ELECTRONICS III	EE3	No	9600	250	0
ANALYST, COMPUTER SYSTEMS II	14102	No	9600	500	0
ANALYST, COMPUTER SYSTEMS III	14103	No	9600	750	0
NAVY VALIDATOR LEVEL II	ILNV2	No	9600	500	0
NAVY VALIDATOR LEVEL III	FQNV3	No	9600	500	0
TECHNICAL WRITER LEVEL I	30461	No	9600	500	0

TECHNICAL WRITER LEVEL III	30463	No	9600	500	0
SPECIALIST, CONFIGURATION MGMT III	SCM3	No	8815	285	0
LOGISTICIAN II	LGT2	No	8815	275	0
ILLUSTRATOR II	13042	No	8815	275	0
LOGISTICIAN III	LGT3	No	9600	500	0
DRAFTER/CAD OPERATOR III	30063	No	8815	265	0
ANALYST, OPERATIONS I	ANP1	No	9600	250	0
MATERIAL COORDINATOR	21030	No	8815	265	0
DATA ENTRY OPERATOR II	01052	No	9600	250	0

Key Personnel

The Contractor shall provide individuals to fill the key positions identified below:

Program/Project Manager II (one resume required):

Target Education: Bachelor's level degree in any technical or managerial discipline

Target Experience: Ten (10) years of professional experience in program/project management

Non-Key Personnel

Although resumes for "Non-Key Personnel" are not required, offerors must fully demonstrate their ability to provide the non-key personnel listed below who meet the requirements that follow. The Contractor shall provide a statement as to their ability to supply the non-key personnel with the experience required to perform the efforts specified in this SOW. The Contractor shall provide individuals to fill the non-key positions identified below:

Analyst, Management II

Minimum Education: Bachelor of Science degree in Business or technical field.

Minimum Experience: Seven (7) years of experience in engineering/science management, operations research analysis or financial/cost analysis.

Engineer, Computer II:

Minimum Education: Bachelor's level degree in Computer, Electrical or Electronics Engineering or Mathematics with field of concentration in computer science.

Minimum Experience: Three (3) years of professional experience in computer design, software development or computer networks

Engineer, Systems II

Minimum Education: Bachelor of Science degree in Computer Science, engineering, information technology, or a related field.

Minimum Experience: Five (5) years of experience in designing computer systems, integrating computer hardware, software, building computers, designing network systems.

Engineer, Mechanical III

Minimum Education: Bachelor's degree in Engineering or Science degree

Minimum Experience: Six (6) years of experience in design, operation, maintenance, testing of Naval Ship Combat Systems, Naval Ships Hull, Deck Machinery Systems, working knowledge of Navy data systems, knowledge of Navy Procedures for maintaining equipment requirements.

Engineer, Design III

Minimum Education: Bachelor of Science degree in Engineering or Industrial Design.

Minimum Experience: Seven (7) years of professional experience in mechanical, structural or electrical/electronic design.

Computer Operator I:

Minimum Education: Associate Degree from accredited University or CNSSI 4011/4012 Certificate.~~High School/Vocational School diploma or GED Certificate~~

Minimum Experience: One (1) years of experience resolving common equipment operating problems.

Computer Operator II:

Minimum Education: Associate Degree from accredited University or CNSSI 4011/4012 Certificate.
~~High School/Vocational School diploma or GED Certificate~~

Minimum Experience: Three (2) years of experience resolving difficult operating problems.

Computer Operator III:

Minimum Education: Associate Degree from accredited University or CNSSI 4011/4012 Certificate.
~~High School/Vocational School diploma or GED Certificate~~

Minimum Experience: Three (3) years of experience resolving high priority operating problems.

Computer Operator IV:

Minimum Education: Associate Degree from accredited University or CNSSI 4011/4012 Certificate.
~~High School/Vocational School diploma or GED Certificate~~

Minimum Experience: Four (4) years of experience resolving complex operating problems.

Computer Operator V:

Minimum Education: Bachelor or Graduate Degree from Accredited University or CNSSI or NTSSI 4015 or 4016GSEC or CISSP or CISM or GSLC or ENSA, Program Management Professional (PgMP).

Minimum Experience: Five (5) years of experience resolving mission critical operating problems.

Manager, Program/Project I

Minimum Education: Bachelor's Degree from an accredited college or university.

Minimum Experience: Four (4) years of professional experience in program/project management.

Technician, Engineering II

Minimum Education: Bachelor Degree from accredited University or CNSSI 4012-4016 Certificate or NDU CISO certificate.
~~Graduate of high school, trade or industrial school or GED equivalent.~~

Minimum Experience: Two (2) years of engineering experience in the operation, test and maintenance of naval ship Combat Systems, Hull, Mechanical, Electrical, Electronic, equipment and systems. Experience must include use of naval ship blueprint and technical manual documentation.

Technician, Engineering III

Minimum Education: Bachelor Degree from accredited University or CNSSI 4012-4016 Certificate or NDU CISO certificate.
~~Graduate of high school, trade or industrial school or GED equivalent.~~

Minimum Experience: Three (3) years of engineering experience in the operation, test and maintenance of naval ship Combat Systems, Hull, Mechanical, Electrical, Electronic, equipment and systems. Experience must include use of naval ship blueprint and technical manual documentation.

Technician, Engineering IV

Minimum Education: Bachelor Degree from accredited University or CNSSI 4012-4016 Certificate or NDU CISO certificate.
~~Graduate of high school, trade or industrial school or GED equivalent.~~

Minimum Experience: Four (4) years of engineering experience in the operation, test and maintenance of naval ship Combat Systems, Hull, Mechanical, Electrical, Electronic, equipment and systems. Experience must include use of naval ship blueprint and technical manual documentation.

Engineer, Systems IV

Minimum Education: Bachelor's level degree in Computer, Electrical or Electronics Engineering or Mathematics with field of concentration in computer science

Minimum Experience: Four (4) years of professional experience in systems engineering.

Engineer, Design IV

Minimum Education: Bachelor of Science degree in Engineering or Industrial Design.

Minimum Experience: Ten (10) years of professional experience in mechanical, structural or electrical/electronic design.

Engineer, Electrical/Electronics III

Minimum Education: Bachelor of Science degree in Electrical/Electronics Engineering.

Minimum Experience: Seven (7) years of professional experience in the design, development, testing, and supervision of the manufacturing of electrical and electronic equipment.

Analyst, Computer Systems II:

Minimum Education: Bachelor Degree from Accredited University or CNSSI 4012 or 4013 or 4014 or 4015 or 4016 Certificate or NDU CISO certificate or CCNA or CAP or Security + (CE) or ENSA.

Minimum Experience: Four (4) years professional experience in computer systems analysis.

Analyst, Computer Systems III:

Minimum Education: Bachelor Degree from Accredited University or CNSSI 4012 or 4013 or 4014 or 4015 or 4016 Certificate or NDU CISO Certificate CCNA or CAP or Security + (CE) or ENSA.

Minimum Experience: Seven (7) years professional experience in computer systems analysis.

Navy Validator II:

Minimum Education: Bachelor's degree in computer science or related IT field.

Minimum Experience: Four (4) years IA or A&A experience, completed Department of the Navy (DON) and Risk Management Framework (RMF) Validator training course. Hold active Navy Validator Level II Credentials.

Navy Validator III:

Minimum Education: Master's degree in computer science or IT related field.

Minimum Experience: Seven (7) years IA or A&A experience, completed Department of the Navy (DON) and Risk Management Framework (RMF) Validator training course. Hold active Navy Validator Level III Credentials.

Technical Writer I

Minimum Education: Bachelor Degree from Accredited University or CNSSI 4012 or 4013 or 4014 or 4015 or 4016 Certificate or NDU CISO certificate CCNA or CAP or Security + (CE) or ENSA.

Minimum Experience: Two (2) years of professional experience in technical writing/editing.

Technical Writer III

Minimum Education: Bachelor Degree from Accredited University or CNSSI 4012 or 4013 or 4014 or 4015 or 4016 Certificate or NDU CIO certificate; CISSP or CISM or GSLC or CASP.

Minimum Experience: Two (4) years of professional experience in technical writing/editing.

Specialist, Configuration Management III

Minimum Education: Bachelor's degree in any field.

Minimum Experience: Ten (10) years of experience in managing, performing quality assurance, control inspections on naval ship software including Combat Systems, Hull, Mechanical, Electrical and Electronic systems.

Logistician II

Minimum Education: Graduate of high school, trade or industrial school or GED equivalent.

Minimum Experience: Four (4) years of professional experience in integrated logistics support.

Illustrator II

Minimum Education: Graduate trade or industrial school in Illustrating, Graphic Arts or Drafting.

Minimum Experience: Five (5) years of professional experience in illustrating.

Logistician III

Minimum Education: Graduate of high school, trade or industrial school or GED equivalent.

Minimum Experience: Seven (7) years of professional experience in integrated logistics support.

Drafter/CAD Operator III

Minimum Education: Graduate from an accredited technical, vocational, or apprentice school drafting program.

Minimum Experience: Five (5) years of experience including use of AUTOCAD Release 10 and 12 and/or one (1) year of experience including use of ISODRAW Release 5.0.

Analyst, Operations I

Minimum Education: Associate of Science degree in Engineering, Physics or Mathematics.

Minimum Experience: Three (3) years of professional experience in coordination, operations and research.

Material Coordinator

Minimum Education: Graduate of high school, trade or industrial school or GED equivalent.

Minimum Experience: Five (5) years of professional experience in coordination of material, parts, and assemblies within or between departments.

Data Entry Operator II:

Minimum Education: High school/vocational diploma or GED certificate

Minimum Experience: One (1) year of professional experience in searching for, interpreting, selecting, and coding items from a variety of source documents.

16.1 DON Cyberspace IT (Information Technology) / Cybersecurity & Information Assurance Functions and Personnel Requirements

In accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program, and SECNAV 5239.2, DON IAWF Management Manual to support the Cybersecurity/IAWF Program, Contractors performing IA functions must be designated as a member of the Cybersecurity\IA Workforce. Personnel designated shall meet qualification requirements for their duties, which may include both an IA baseline certification and operating system (OS)/Computing Environment (CE) certification requirement per below instructions:

16.1.1 Contractors performing Cybersecurity/IA functions must meet the minimum IA baseline certification prior to being engaged as defined in the CSWF Matrix below.

16.1.2 Contractor personnel agree as a "condition of employment" to obtain (and maintain) the appropriate certifications and continuing profession education requirements for their Cybersecurity/IAWF position.

16.1.3 Contractor personnel accessing information systems shall meet applicable training and certification requirements set forth in DoD 8570.01M and SECNAV M-5239.2. The contractor is responsible to ensure that personnel possess and maintain the proper and current Information Assurance (IA) certifications in accordance with DoD 8570.01M and the Computing Environment/Operating System (CE/OS) certifications in accordance with the CSWF Matrix below.

16.1.4 Upon hire all contractor personnel assigned to the IAM/IAT Level I-III position (as appropriate) shall sign the Information System Privileged Access Agreement and Acknowledgement of Responsibilities statement.

16.1.5 Cybersecurity/IA Workforce labor categories are identified herein. The Contractor shall ensure that personnel have the proper and current information assurance certification to perform information assurance functions in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program. The Contractor shall meet the applicable information assurance certification requirements, including-

16.1.6 DoD-approved information assurance workforce certifications appropriate for each category and level as listed in the current version of DoD 8570.01-M; and

16.1.7 Appropriate operating system certification for information assurance technical (IAT) positions as required by DoD 8570.01-M.

16.1.8 The Contractor shall provide the current information assurance certificates and or documentation supporting IA certification and current status of personnel performing Cybersecurity/IA duties. Baseline and Operating System (OS) Certification requirements listed in the CSWF Matrix must be met and are a condition of hire.

16.1.9 The contractor shall ensure that cybersecurity/IA contractor personnel are appropriately certified and maintain current Continuing Professional Education (CPE) requirements as a condition of employment.

16.1.10Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions.

Information assurance contractor training and certification-

16.1.11Continuing Professional Education (CPE) requirements are not a direct contractor cost to the Government. The contractor is responsible for meeting the qualification requirements for all positions on the contract in the Cybersecurity Workforce Certification Matrix (CSWF) as shown below, and shall not invoice the Government for training, certification tests, or continuing profession education requirements.

Table 1 – CyberSecurity WorkForce (CSWF) Certification Matrix

Task Area	**Labor Category**	**Specialty Code**	**Proficiency Level**	**Baseline Qualification**	**Operating System/ Computing Environment (OS/CE) Qualification**	**Continuing Professional Education (CPE) Req'ts**
Project Management Categories						
	MANAGER, PROGRAM/PROJECT II	75	Intermediate/ Journeyman	Bachelor Degree from accredited University or CNSSI 4012 or 4013 or 4013 or 4014 or 4015 or 4016 Certificate or NDU CISO certificate or AQD GA7;	Directed by the Privileged Access Agreement	40 CPEs annually

				CCNA or CAP or Security + (CE) or Program Management Professional (PgMP)		
	ANALYST, MANAGEMENT II	75	Intermediate/Journeyman	Bachelor Degree from accredited University or CNSSI 4012 or 4013 or 4013 or 4014 or 4015 or 4016 Certificate or NDU CISO certificate or AQD GA7; CCNA or CAP or Security + (CE) or Program Management Professional (PgMP)	Directed by the Privileged Access Agreement	40 CPEs annually
	ENGINEER, SYSTEMS II	67	Intermediate/ Journeyman	Bachelor Degree from accredited University or CNSSI 4012-4016 Certificate or NDU CISO certificate; CCNA or CAP or Security + (CE)	Directed by the Privileged Access Agreement	40 CPEs annually
Engineering (Non-Cyber) Related Categories						
	ENGINEER, MECHANICAL III	NA	NA	NA	NA	NA
	ENGINEER, DESIGN III	NA	NA	NA	NA	NA
Research, Development and Cyber Related Categories						
	COMPUTER OPERATOR I	46	Intermediate/ Journeyman	Associate Degree from accredited University or CNSSI 4011/4012 Certificate; CASP or CAP or Security Plus or SSCP, Program Management Professional (PgMP)	Directed by the Privileged Access Agreement	40 CPEs annually

	COMPUTER OPERATOR II	46	Intermediate/ Journeyman	Associate Degree from accredited University or CNSSI 4011/4012 Certificate; CASP or CAP or Security Plus or SSCP, Program Management Professional (PgMP)	Directed by the Privileged Access Agreement	40 CPEs annually
	COMPUTER OPERATOR III	46	Intermediate/ Journeyman	Associate Degree from accredited University or CNSSI 4011/4012 Certificate; CASP or CAP or Security Plus or SSCP, Program Management Professional (PgMP)	Directed by the Privileged Access Agreement	40 CPEs annually
	COMPUTER OPERATOR IV	46	Intermediate/ Journeyman	Associate Degree from accredited University or CNSSI 4011/4012 Certificate; CASP or CAP or Security Plus or SSCP, Program Management Professional (PgMP)	Directed by the Privileged Access Agreement	40 CPEs annually
	COMPUTER OPERATOR V	46	Advanced/Master	Bachelor or Graduate Degree from accredited University or CNSSI or NTSSI 4015 or 4016GSEC or CISSP or CISM or GSLC or ENSA, Program Management Professional (PgMP)	Directed by the Privileged Access Agreement	40 CPEs annually
Shipboard Alteration Related Categories						
	MANAGER, PROGRAM/PROJECT I	N/A	N/A	N/A	N/A	N/A

	TECHNICIAN, ENGINEERING II	67	Intermediate/ Journeyman	Bachelor Degree from accredited University or CNSSI 4012-4016 Certificate or NDU CISO certificate; CCNA or CAP or Security + (CE)	Directed by the Privileged Access Agreement	40 CPEs annually
	TECHNICIAN, ENGINEERING III	67	Intermediate/ Journeyman	Bachelor Degree from accredited University or CNSSI 4012-4016 Certificate or NDU CISO certificate; CCNA or CAP or Security + (CE)	Directed by the Privileged Access Agreement	40 CPEs annually
	TECHNICIAN, ENGINEERING IV	67	Advanced/Master	Graduate Degree from accredited University or CNSSI 4012-4016 Certificate or NDU CIO certificate; CISSP or CISM or GSLC or CASP	Directed by the Privileged Access Agreement	40 CPEs annually
Research, Development and Cyber Related Categories						
	ENGINEER, COMPUTER II	67	Intermediate/ Journeyman	Bachelor Degree from accredited University or CNSSI 4012-4016 Certificate or NDU CISO certificate; CCNA or CAP or Security + (CE)	Directed by the Privileged Access Agreement	40 CPEs annually
	ENGINEER, SYSTEMS IV	67	Advanced/ Master	Graduate Degree from accredited University or CNSSI 4012-4016 Certificate or NDU CIO certificate; CISSP or CISM or GSLC or CASP	Directed by the Privileged Access Agreement	40 CPEs annually
		67	Intermediate/	Bachelor Degree from accredited University or	Directed by the Privileged	40 CPEs annually

	ENGINEER, DESIGN IV		Journeyman	CNSSI 4012-4016 Certificate or NDU CISO certificate; CCNA or CAP or Security + (CE)	Access Agreement	
	ENGINEER, ELECTRICAL/ELECTRONICS III	67	Intermediate/ Journeyman	Bachelor Degree from accredited University or CNSSI 4012-4016 Certificate or NDU CISO certificate; CCNA or CAP or Security + (CE)	Directed by the Privileged Access Agreement	40 CPEs annually
	ANALYST, COMPUTER SYSTEMS II	61	Intermediate/ Journeyman	Bachelor Degree from accredited University or CNSSI 4012 or 4013 or 4014 or 4015 or 4016 Certificate or NDU CISO certificate; CCNA or CAP or Security + (CE) or ENSA	Directed by the Privileged Access Agreement	40 CPEs annually
	ANALYST, COMPUTER SYSTEMS III	61	Intermediate/ Journeyman	Bachelor Degree from accredited University or CNSSI 4012 or 4013 or 4014 or 4015 or 4016 Certificate or NDU CISO certificate CCNA or CAP or Security + (CE) or ENSA	Directed by the Privileged Access Agreement	40 CPEs annually
	NAVY VALIDATOR LEVEL II	61	Entry	A+ (CE) or Network + (CE) or SSCP or Associate Degree from accredited University or CNSSI 4011 Certificate or NEC 2791 (A-150-1980 or K-150-2115) or IP BASIC (CIN: J-3B-0440)	Directed by the Privileged Access Agreement	40 CPEs annually

	NAVY VALIDATOR LEVEL III	61	Intermediate	CCNA or CAP or Security + (CE) or ENSA or Bachelor Degree from accredited University or CNSSI 4012 or 4013 or 4014 or 4015 or 4016 Certificate or NDU CISO certificate or NEC 2780 (CIN: A-531-0022) or 2779 (CIN: A-531-0009) or 2781 (CIN: A-531-0045)	Directed by the Privileged Access Agreement	40 CPEs annually
	TECHNICAL WRITER LEVEL I	61	Intermediate/ Journeyman	Bachelor Degree from accredited University or CNSSI 4012 or 4013 or 4014 or 4015 or 4016 Certificate or NDU CISO certificate CCNA or CAP or Security + (CE) or ENSA	Directed by the Privileged Access Agreement	40 CPEs annually
	TECHNICAL WRITER III	61	Advanced/Master	Bachelor Degree from accredited University or CNSSI 4012 or 4013 or 4014 or 4015 or 4016 Certificate or NDU CIO certificate; CISSP or CISM or GSLC or CASP	Directed by the Privileged Access Agreement	40 CPEs annually
Quality Assurance and Logistics Labor Categories						
	SPECIALIST, CONFIGURATION MGMT III	NA	NA	NA	NA	NA
	LOGISTICIAN II	NA	NA	NA	NA	NA
	ILLUSTRATOR II	NA	NA	NA	NA	NA
	LOGISTICIAN III	NA	NA	NA	NA	NA
	DRAFTER/CAD OPERATOR III	NA	NA	NA	NA	NA
	ANALYST, OPERATIONS I	NA	NA	NA	NA	NA

	MATERIAL COORDINATOR	N/A	N/A	N/A	N/A	N/A
	DATA ENTRY OPERATOR II	N/A	N/A	N/A	N/A	N/A

In accordance with Clause 252.239-7001, contractors shall submit the following information for all new contractor employees who will be performing under the above CSWF labor categories 5 days prior to the contractor employee beginning performance: First Name, Last Name, Company Name, Contract #, Labor Category, Supporting NSWCPD Branch, Copy of Certifications and/or Education Transcripts.

17.0OTHER CONDITIONS/REQUIREMENTS

Government sole use and distribution rights. Information given to the contractor during the life of this project must only be used for the purpose of carrying out the performance of this contract. As a condition of satisfactorily performing the contract, the contractor shall forego any rights to distribute, sell, or use for internal purposes, all artifacts developed, compiled and otherwise maintained in the contractor’s or its employees’ possession.

Retention of Contractor Personnel. The contractor shall make every effort to retain personnel in order to ensure continuity until project completion. If it should become necessary to substitute or replace personnel, the contractor shall immediately notify the Government Project Lead and/or COR/Specialist/KO in writing of any potential vacancies. The contractor shall inform the Government of what projects or assignments might be affected with a change in personnel.